3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: 220208-0264]

National Cybersecurity Center of Excellence (NCCoE) *Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems*

AGENCY: National Institute of Standards and Technology, Department of Commerce.

ACTION: Notice.

SUMMARY: The National Institute of Standards and Technology (NIST) invites organizations to provide letters of interest describing products and technical expertise to support and demonstrate security platforms for the *Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems* project. This notice is the initial step for the National Cybersecurity Center of Excellence (NCCoE) in collaborating with technology companies to address cybersecurity challenges identified under the *Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems* project. Participation in the project is open to all interested organizations.

DATES: Collaborative activities will commence as soon as enough completed and signed letters of interest have been returned to address all the necessary components and capabilities, but no earlier than [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: The NCCoE is located at 9700 Great Seneca Highway, Rockville, MD 20850. Letters of interest must be submitted to water_nccoe@nist.gov or via hardcopy to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Interested parties can access the letter of interest request by visiting www.nccoe.nist.gov/projects/securing-water-and-wastewater-utilities and completing the letter of interest webform. NIST will announce the completion of the selection of participants and inform the public that it is no longer accepting letters of interest for this project at www.nccoe.nist.gov/projects/securing-water-and-wastewater-utilities. Organizations whose letters of interest are accepted in accordance with the process set forth in the **SUPPLEMENTARY INFORMATION** section of this notice will be asked to sign an NCCoE consortium Cooperative Research and Development Agreement (CRADA) with NIST. An NCCoE consortium CRADA template can be found at: https://www.nccoe.nist.gov/publications/other/nccoe-consortium-crada-example.

FOR FURTHER INFORMATION CONTACT: James McCarthy via telephone at 301-975-0228; by email at water_nccoe@nist.gov; or by mail to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Additional details about the *Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems* project are available at https://www.nccoe.nist.gov/projects/securing-water-and-wastewater-utilities.

SUPPLEMENTARY INFORMATION:

Background: The NCCoE, part of NIST, is a public-private collaboration for accelerating the widespread adoption of integrated cybersecurity tools and technologies. The NCCoE brings together experts from industry, government, and academia under one roof to develop practical, interoperable cybersecurity approaches that address the real-world needs of complex Information Technology (IT) and Operational Technology (OT) systems. By accelerating dissemination and use of these integrated tools and technologies for protecting IT and OT assets, the NCCoE will enhance trust in U.S. IT and OT communications, data, and storage systems; reduce risk for companies and individuals using IT and OT systems; and encourage development of innovative, job-creating cybersecurity products and services.

Process: NIST is soliciting responses from all sources of relevant security capabilities (see below) to enter into an NCCoE Cooperative Research and Development Agreement (CRADA) to provide products and technical expertise to support and demonstrate security platforms for the *Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems* project. The full project can be viewed at: www.nccoe.nist.gov/projects/securing-water-and-wastewater-utilities.

Interested parties can access the request for a letter of interest template by visiting the project website at www.nccoe.nist.gov/projects/securing-water-and-wastewater-utilities and completing the letter of interest webform. On completion of the webform, interested parties will receive access to the letter of interest template, which the party must complete, certify as accurate, and submit to NIST by email or hardcopy. NIST will contact interested parties if there are questions regarding the responsiveness of the letters of interest to the project objective or requirements identified below. NIST will select participants who have submitted complete letters of interest on a first come, first served basis within each category of product components or capabilities listed below up to the number of participants in each category necessary to carry out this project. When the project has been completed, NIST will post a notice on the *Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems* project website at www.nccoe.nist.gov/projects/securing-water-and-wastewater-utilities announcing the next phase of the project and informing the public that it will no longer accept letters of interest for this project. There may be continuing opportunity to participate even after initial activity commences. Selected participants will be required to enter into an NCCoE consortium CRADA with NIST (for reference, see **ADDRESSES** section above).

Project Objective: This project will develop example cybersecurity solutions to protect the infrastructure in the operating environments of Water and Wastewater Systems (WWS) sector utilities. The increasing adoption of network-enabled technologies by the sector merits the development of best practices, guidance, and solutions to ensure that the cybersecurity posture of facilities is safeguarded.

Critical infrastructure issues in the WWS sector present several unique challenges. Utilities in the sector typically cover a wide geographic area regarding piped distribution networks and infrastructure together with centralized treatment operations. The supporting operational technologies (OT) underpinning this infrastructure are likely reliant on supervisory control and data acquisition (SCADA) systems which provide data transmission across the enterprise, sending sensor readings and signals in real time. These systems also control the automated processes in the production environment which is linked to the distribution network. Additionally, many OT devices are converging upon information technology (IT) capability with the advent of Industrial Internet-of-Things (IIoT) devices and platforms, such as cloud-based SCADA and smart monitoring.

This project will develop a reference design that demonstrates practical solutions for water and wastewater utilities of all sizes. The reference design will use commercially available products and services to address four WWS cybersecurity challenges: asset management, data integrity, remote access, and network segmentation. The commercial products and services will be integrated into a demonstration of the reference design. The project also initiates a broad discussion with WWS sector stakeholders to identify commercial solution providers.

This project will result in a publicly available NIST Cybersecurity Practice Guide which will include a detailed implementation guide of the practical steps needed to implement a cybersecurity reference design that addresses these challenges.

Requirements for Letters of Interest: Each responding organization's letter of interest should identify which security platform component(s) or capability(ies) it is offering. Letters of interest should not include company proprietary information, and all components and capabilities must be commercially available. Components are listed in section 3 of the *Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems* project description available at: www.nccoe.nist.gov/projects/securing-water-and-wastewater-utilities.

Requested Capabilities

This project will employ products, provided by collaborating vendors, that provide the following cybersecurity capabilities to address the four scenarios described in section 2 of the *Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems* Project Description

- Asset Management: Asset management capabilities discover and identify physical and virtual assets in the OT environment. These assets may be geographically distributed and may be cloud-based. In addition to network-connected assets, these capabilities should provide a means to discover and identify assets connected by low-bandwidth communications channels and disconnected assets. The asset management capability maintains an inventory of known assets which contains information such asset type, product version, and communication protocols used. Asset management capabilities may provide automation to establish and enforce a baseline security posture.
- Data Integrity: Data integrity capabilities protect data and communications within the OT environment against improper modification or destruction. Additionally,

these capabilities monitor the OT environment to detect potential integrity violations and generate alerts to initiate any needed responses.

- Remote Access: Remote access capabilities provide entities (people and systems) controlled access to OT assets from outside the OT environment. These capabilities authenticate any entity seeking access, allow only explicitly authorized access, control which actions are allowed for each authorized entity, and maintain a record of all actions attempted and completed by each entity.
- Network Segmentation: Network segmentation capabilities provide logically isolated network subsets that can be managed more efficiently and effectively. Segmentation allows for a more detailed level of authorization and access, visibility into network flows among critical assets and infrastructure, and control of device management, and minimizes the potential harm from threats by isolating them to a limited part of the network.

In their letters of interest, responding organizations need to acknowledge the importance of and commit to provide:

1. Access for all participants' project teams to component interfaces and the organization's experts necessary to make functional connections among security platform components.
2. Support for development and demonstration of the *Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems* project, which will be conducted in a manner consistent with the following standards and guidance: FIPS 200, FIPS 201, SP 800-82 and SP 800-53, the NIST Cybersecurity Framework, and the NIST Privacy Framework.

Additional details about the *Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems* project are available at www.nccoe.nist.gov/projects/securing-water-and-wastewater-utilities.

NIST cannot guarantee that all the products proposed by respondents will be used in the demonstration. Each prospective participant will be expected to work collaboratively with NIST staff and other project participants under the terms of the NCCoE consortium CRADA in the development of the *Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems* project. Prospective participants' contribution to the collaborative effort will include assistance in establishing the necessary interface functionality, connection and set-up capabilities and procedures, demonstration harnesses, environmental and safety conditions for use, integrated platform user instructions, and demonstration plans and scripts necessary to demonstrate the desired capabilities. Each participant will train NIST personnel, as necessary, to operate its product in capability demonstrations. Following successful demonstrations, NIST will publish a description of the security platform and its performance characteristics sufficient to permit other organizations to develop and deploy security platforms that meet the security objectives of the *Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems* project. These descriptions will be public information. Under the terms of the NCCoE consortium CRADA, NIST will support development of interfaces among participants' products by providing IT infrastructure, laboratory facilities, office facilities, collaboration facilities, and staff support to component composition, security platform documentation, and demonstration activities.

The dates of the demonstration of *Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems* project capability will be announced on the NCCoE website at least two weeks in advance at https://nccoe.nist.gov/. The expected outcome will demonstrate how the components of the *Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems* project architecture can provide security capabilities to mitigate identified risks related to data throughout its lifecycle. Participating organizations will gain from the knowledge that their products are interoperable with other participants' offerings.

For additional information on the NCCoE governance, business processes, and NCCoE operational structure, visit the NCCoE website https://nccoe.nist.gov/.

Alicia Chambers,
NIST Executive Secretariat.

[FR Doc. 2023-13043 Filed: 6/16/2023 8:45 am; Publication Date: 6/20/2023]